MANAGEMENT

CHAPTER 9

(FILE NAME ON DISK # 1 = S2C9.WPD)

Information processing in financial institutions has experienced rapid change, because of new and enhanced information systems (IS) and technology. These new technologies enable institutions to move data processing resources from centralized mainframe computers to end-user computing systems and distributed processing networks throughout the organization. Third party vendors are also offering a variety of financial products and services to replace or supplement in-house information systems. As a result, a financial institution's IS processing may be performed by a combination of mainframe computer systems, service bureaus, and end-user computing systems. Because of this changing environment, agency and industry emphasis is shifting from the management of data centers to the management of information systems and technology. The FFIEC member agencies recognize this shift from the review of the traditional computer center to that of information systems technology throughout the enterprise. The FFIEC is addressing this shifting focus from a departmental review to an enterprise IS review. The examination approach, scope, and procedures must provide for the effective review of the institution's information systems processing environment.

The management concepts discussed in this section apply to all types of information systems organizations. Data processing services may be provided by a department(s) of the financial institution, a financial institution holding company subsidiary, or an independently owned and operated data center. In this section the term information systems refers to each of these entities.

MANAGEMENT

A review of the management of information systems should determine if it is current and addresses the major technology-related challenges, issues, and problems facing the institution. This includes, but is not limited to, the need for effective procurement and deployment of technology, protection of assets through corporate security and contingency planning, and maintenance of the delivery technology infrastructure through architecture and interfaces. Managing information systems and technology increasingly involves joint cooperative efforts throughout the institution. As a result, the IS examination effort is challenged to study and review an organization's interdependent operations, including the data centers, networks, and user operations.

A review of IS management should determine if it is properly organized, has qualified personnel, and appropriate controls in place. To evaluate whether management is properly organized, reviewers must determine if:

- The management oversight structure is effective (responsibilities may be shared between centralized and decentralized user and outsourced activities).
- The corporate IS policies and standards are well-defined by management and the board of directors. The institution should have an organization chart and policies that specifically define lines of authority and responsibilities for each IS function.

In reviewing IS management, the examiner must determine whether proper and effective supervision and internal controls are implemented and maintained to ensure the integrity of financial reporting and management information systems (MIS). Examiners should also ensure that the MIS meet the decision and reporting needs of the organization. Basic internal control principles, such as segregation of duties, dual custody, and audit trails, are key elements in information systems control. Management also must provide an adequate continuing education program for IS personnel.

ORGANIZATION

The IS function is an inherent part of the financial institution's organizational structure. The function(s) can be centralized in the institution. The senior IS manager should report to the highest level of institution management. An IS steering committee comprised of senior management, is usually formed to provide direction.

The board of directors approves IS plans, policies, and major expenditures, and board members should be familiar with information systems and data center concepts and activities. Senior management must ensure that the board's policies are followed and that the IS function(s) meets the needs of the organization. IS management supervises the day-to-day activities that require a high level of technical proficiency.

Detailed information on organizational structure is essential to review the IS function adequately. The structure and supervision should be evaluated to determine if lines of authority provide for an effective separation of duties.

Organization Charts

The independence of the IS function(s) relative to others can be determined by reviewing the institution's organization chart. Examiners should consider lines of authority and separation of duties. Effective organization charts should graphically illustrate function, the current lines of authority and responsibility. Adequate supervision and segregation of duties should also be evident. Overlapping responsibilities should be questioned, i.e., programmers with computer operator duties or user department managers also in charge of data center operations. Figures 9.1, 9.2, and 9.3 contain sample organization charts. IS organizations have certain characteristics depending upon their size:

- The "small" IS organization chart (Figure 9.1) represents a small holding company or financial institution with an in-house computer. These organizations usually lack an internal programming function. Programming activities are limited, and the software vendor may provide program changes and revisions. An IS management function, such as the one depicted in Figure 9.1, may or may not exist in a smaller institution. Communication tends to be informal and verbal. A complete separation of duties may not be economically feasible. Compensating controls may include cross-training of personnel, dual control over sensitive material, rotation of duties, and independent reviews and audits.

- In "medium-sized" IS organizations with a large number of users (Figure 9.2), the structure is usually more formal. Senior management and the board of directors must be informed of IS activities. End-user computer systems are frequently processing significant applications. This type of organization has a more defined separation of duties than smaller IS ones.

- "Large" IS organizations (Figure 9.3) should have detailed organization charts and position descriptions. They also should have steering committees and regularly scheduled management meetings to enhance communication and monitor activities. Large IS organizations often have multiple data centers and end-user computer systems that operate independently. These independent systems generally are structured as small-sized IS organizations that use microcomputers to process significant applications.

Position Descriptions

Responsibilities should be defined for each data processing function. Usually, they are determined by IS management and tailored to the department's size and complexity. Responsibility, accountability, and reporting authority can be defined through position descriptions. They provide an objective means of measuring job performance when employees understand management's expectations. Position descriptions and terminology may vary considerably among organizations. The following descriptions provide examples of typical positions that may be found in an IS organization. Not all positions may be present in every organization or several positions may be performed by one person.

Information Systems Manager – Supervises the resources and activities of the IS function, department, or subsidiary; coordinates services between the data processing area and other user departments and reports to senior management on the plans, projects, performance, and matters relating to

information systems.

Operations Manager – Responsible for computer center(s) operation including construction, equipment installation, maintenance, and personnel; Coordinates the daily activities of the computer installation(s); monitors current production to ensure adherence to established schedules. Redirects workflow when processing is interrupted; and provides for cross-training and rotation of personnel.

Operations Shift Supervisor – Coordinates operation of computer equipment during each shift; monitors computer operation and handles most routine problems; may also be responsible for job scheduling.

Figure 9.1
Sample Organization Chart: Small IS Organization

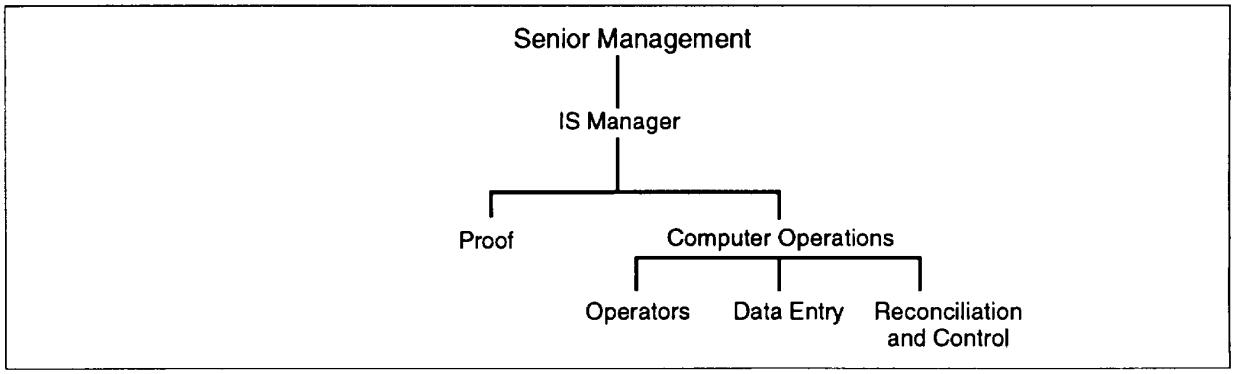


Figure 9.2
Sample Organization Chart: Medium IS Organization

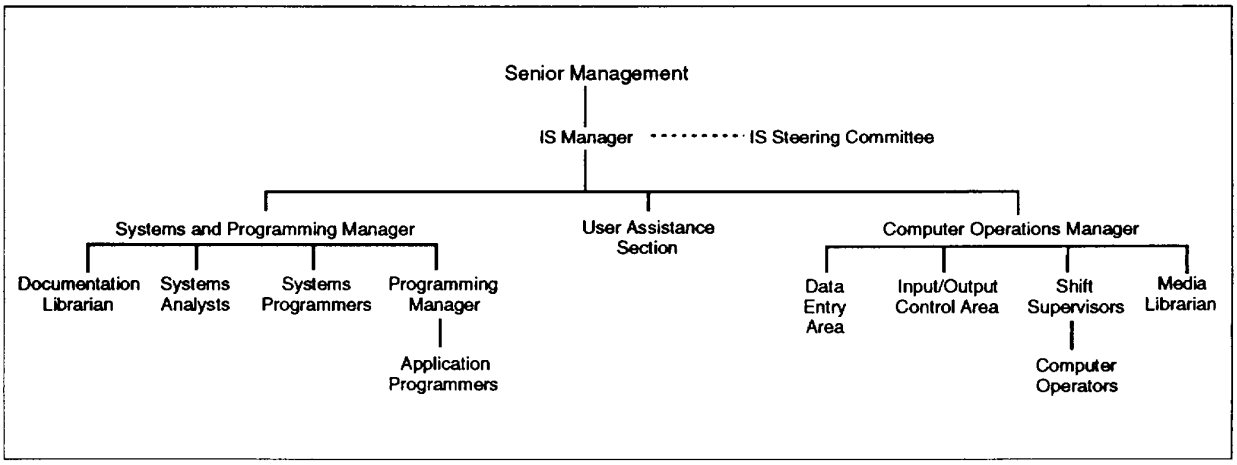
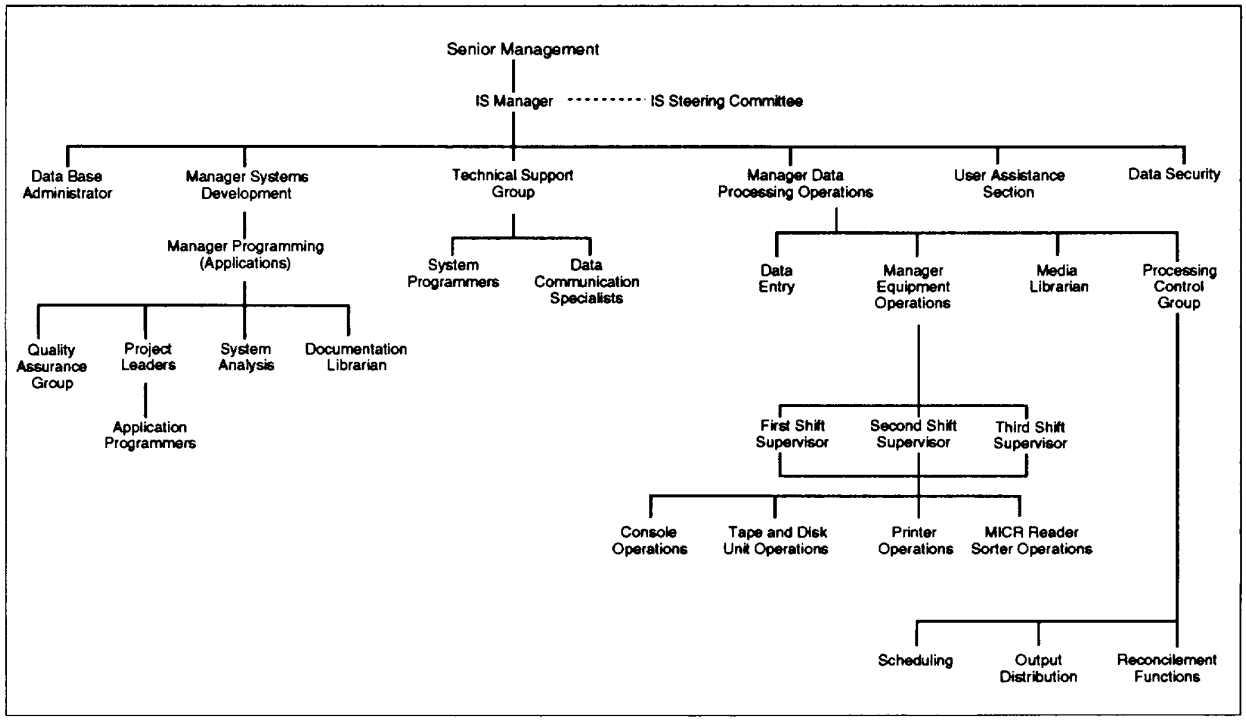


Figure 9.3
Sample Organization Chart: Large IS Organization



Computer Operator – Operates computer hardware according to instructions in Operator's Run manuals. Large installations may have designated operators for computer console, disk and tape drives, and printers. Regardless of the scope of their duties, operators' functions should be limited to those contained in the run manuals for equipment they operate. Operators should not perform any programming or librarian functions and should have access only to documentation necessary to run a given program.

Media Librarian – Has physical control and safekeeping of the center's machine-readable data files and computer programs; also responsibility for accurate disk and tape inventories and for appropriate control and filing of data files. Releases the necessary files for computer production or test runs; maintains accurate records of library activities; ensures that the remote backup library contains appropriate files and is subject to adequate physical control.

Input Preparation Personnel

Proof Operator – Balances and proves the work received from branches, departments, and outside companies; and derives control totals by category for entry into the processing environment.

High Speed Reader/Sorter Operator – Operates equipment which captures the magnetic ink character recognition (MICR) information on documents, converts the information into machine-readable form, and sorts the documents and checks.

Data Entry Operator – Prepares and enters data for processing via terminals or key-to-disk or tape units.

Output Personnel

Reconcilement Staff – Validates accuracy and accountability of transactions; reconciles all output to input control totals; prepares rejected/non-read items for re-entry and makes final reconcilement; and completes user-submitted reconcilement forms to reflect accurate capture or note differences and out-of-balance conditions.

Distribution Staff – Ensures that output is routed and distributed to assigned destinations.

Systems and Programming Personnel

Systems and Programming Manager – Supervises systems and programming staff and coordinates all systems development and programming work for mainframe and PC-based systems; establishes or implements programming and other departmental procedures and is responsible for programming related projects, including measurement of progress relative to predetermined goals and schedules.

Systems Analyst – Analyzes requirements for information processing; evaluates the existing automated systems and designs new or revised procedures for accomplishing the activity; provides the interface between the user of the system and the IS technicians who design it; designs program logic, application system flowcharts, and narratives.

Programmer – Creates and modifies programs and program documentation; converts the program logic into coding suitable for entry into computer equipment; and corrects errors in logic or coding (debugging). The general term "programmer" may be further subdivided into systems programmers and applications programmers:

Systems Programmer – Develops and maintains operating system programs that are necessary for the computer equipment to function, but do not directly perform a production task (such as demand deposit accounting); Usually are responsible for maintaining sophisticated file management routines, data base systems, and large telecommunication networks; Generates, develops, and maintains the operating system; Maintains utilities, job control language, input/output control programs, and control modules; and may develop programs that monitor and measure the performance of the operating system and application programs.

Applications Programmer – Translates instructions from systems analysts to computer requirements and develops, tests, and documents programs that produce the desired actions or products; designs detailed flowcharts, verifies program logic by preparing test data for trial runs, revises and refines programs, and documents all procedures used in finished programs. at a junior level codes, prepares different levels of block diagrams and flowcharts, debugs programs, and assists in various non-critical areas. Has overall responsibility for development, testing, and maintenance of application programs.

Telecommunications Support Manager – Supervises the planning, installation, and testing of telecommunications systems for local and wide-area networks; Directs staff of computer specialists for support of telecommunications resources of organization.

Documentation Librarian – Controls and distributes documentation relating to computer programs; generally reviews documentation of new operating systems and applications to ensure completeness and compliance with standards; and ensures that documentation is updated when modifications are made to existing systems and application programs.

Security Officer – Responsible for the physical and logical security of IS resources and assets; and performs risk analysis to determine the exposures and threats to the computer resources and coordinates with IS and user departments to establish appropriate controls to safeguard resources and assets.

User Assistance Staff – Act as liaison between the computer operation and user departments; provides explanations of output reports generated for user purposes (user reports); and develops technical information, describing input documents and output reports (e.g., user manual).

Technical Support Staff – Act as liaison with computer manufacturer, software support personnel (customer engineers), applications programmers, and systems analysts; and oversees systems development between programming and IS operations; This function usually consists of one or more systems programmers with high technical knowledge.

Network Services Support Staff – Act as liaison with software support and operations personnel to assure a proper and effective on-line communication network. This function is usually staffed with people with data communications and network expertise.

Data Base Administrator – Acts as the clearinghouse and guardian for any requests to change data

representation, deletes data elements (a category of data), or modifies data base access security. This person or group is responsible for the organization of and software security controls over data maintained in a data base file structure.

Quality Assurance Staff – Responsible for reviewing the progress of systems development projects to determine conformity to the installation's standards and procedures. Projects that are substantive in development cost, profit impact, or risk should be reviewed by this group to assure a quality product.

PLANNING

The term "planning" implies preparing for future activities by defining goals and the strategies used to achieve them. Information systems are an integral part of financial institution operations. IS resources must be integrated into the overall management or business planning process. Major investments in IS resources have long-term implications on both the delivery and performance of automated products and services. Independent data centers also must plan effectively, so that they can provide quality and cost-effective service to client financial institutions. Institution management should monitor the strategies and plans of independent data centers that provide services.

Plans may vary significantly depending on the size and structure of the organization. Formal plans should be measured by whether the specific plan being reviewed meets the organization's near term and long range needs. A good plan requires that the board of directors, senior management, and users are involved in the planning process. The board of directors must review and approve the plan. Senior management participates in formulating and implementing it after approval by the board of directors. The individual departments and functional areas, carry out the plan.

Planning can be divided into strategic or long-term planning, and operational or short-term planning, as follows:

- Strategic planning focuses on the long-term use of IS resources to achieve corporate goals. A strategic plan should address long-term goals and outline specific steps and timetables to achieve them. It should include hardware and software architecture, end-user computing resources, and any processing done by outside vendors. The plan should address IS resources for an institution and include a budget(s), periodic reporting of capital expenditures to the board and appropriate committees, and disaster/contingency planning. The final plan should be approved by the board and reviewed periodically to ensure IS performance is consistent with the plan (see Chapter 25, FFIEC issuance SP-7: Interagency Policy on Strategic Information Systems Planning for Financial Institutions).

- Operational planning focuses on short-term actions, e.g., annual planning. The operational plans should flow logically from the strategic plan and be revised at least annually.

An effective planning process may include:

- Developing a mission.
- Evaluating the institution's information systems and technology.
- Assessing the present and future information systems environments.
- Formulating goals.
- Allocating resources.
- Implementing plans.
- Analyzing results.
- Revising the plan.

Financial institutions may differ in the thoroughness and degree of planning. The complexity of operations will determine the formality of the planning process for a particular institution. Plans should always be documented and communicated to the appropriate parties. However, in a small community financial institution, the absence of a written plan does not mean management and the board have neglected planning for the future. For institutions lacking a written plan, the examiner should obtain the information through interviews. Written plans are desirable, but they do not guarantee that an effective

planning process exists. The examiner should evaluate the process as well as the written product.

Critical Factors

The formality and complexity of IS plans, depends on the size of the financial institutions. However, an IS plan should consider the following critical areas in all institutions:

- *Applications software* – Includes changes in software used to provide financial services and products, because of competition, market forces, and changing regulations. These changes may require enhancements to, or replacements of, application software for mainframe and end-user computing systems. Management must anticipate these changes in planning future requirements.

- *Operating software* – Includes operating systems, compilers and utilities that are designed to enable the equipment and applications software to function effectively. Changes in this area can have major impact on hardware and software specifications.

- *Hardware* – Consists of mainframes, minicomputers, microcomputers, communications networks, and peripherals. Planning must ensure that the mainframe and end-user computing equipment has sufficient capacity to meet current needs and future growth. For example, planning may indicate that economically it is impractical to add new mainframe equipment. Rather, it may be appropriate to allow a department to purchase a microcomputer or minicomputer and to operate independently of the main data center.

- *Personnel* – Includes staff changes, scheduling requirements, training, and compensation. Planning should consider whether inadequate salaries could cause high employee turnover or if excessive salaries could suppress earnings.

- *Budget* – Consists of quantifying the financial requirements of the plan. Considerations include, but are not limited to, the potential costs for new applications software, new equipment, and staffing changes.

Information Systems Steering Committee

A management group should oversee the IS planning process. This group may have one of many titles, such as IS Steering Committee, IS Operations Committee, or IS Management Committee. In smaller institutions, the entire board may fill this function. In all cases, a charter defining the role and responsibilities of the committee, and its frequency of meetings, should be developed and ratified by the board of directors. This committee mainly oversees the development and maintenance of the IS strategic plan. It should consist of representatives of senior management, the information systems department, and major end user departments. Internal audit should participate in an advisory, nonvoting capacity.

The committee's duties and responsibilities should be defined in a formal charter. Members do not have to be department heads, but should know IS department policies, practices, and procedures. Each member should have the authority to make decisions within the group for their respective areas.

Such committees typically serve as a general review board for major IS projects and should not become involved in routine operations. They perform the following functions:

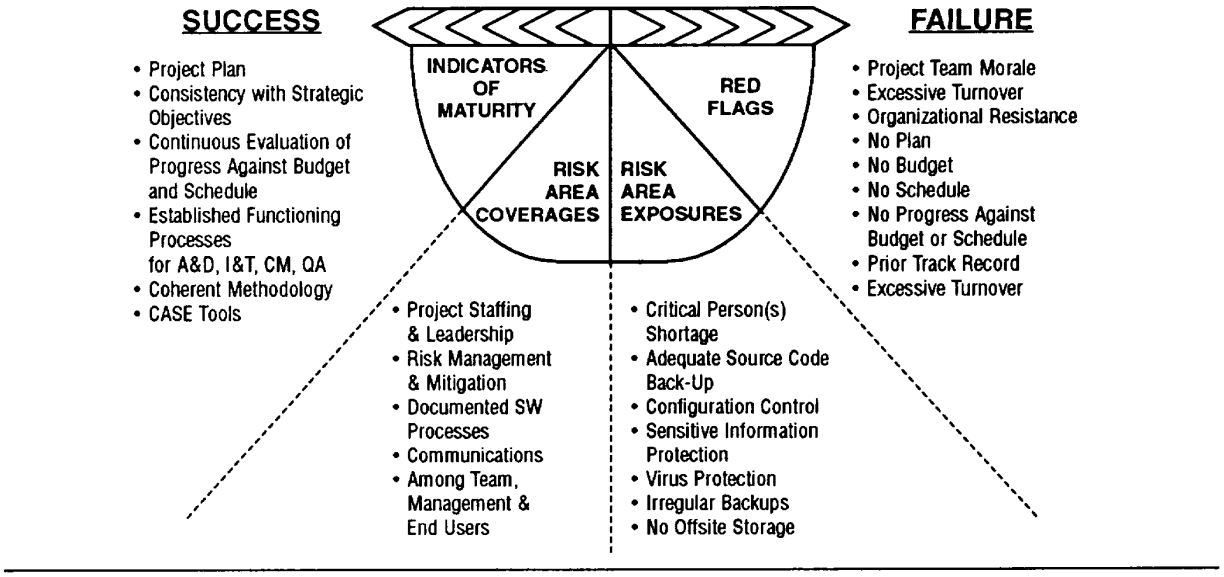
- Review and approve major acquisitions of hardware and software within limits approved by the board of directors.

- Approve and monitor major projects, establish priorities, approve standards and procedures, and monitor overall IS performance.

- Provide liaison between the IS department and user departments.

- Review and approve major IS capital expenditures within board approved limits.
- Approve and monitor major projects, the status of IS plans, and annual budgets.
- Review adequacy of resources and allocation of resources in terms of time, personnel, and equipment.

Figure 9.4
Assessing the Likelihood of Success or Failure



With Permission M. Zola Rapid Systems Solutions, Inc.

The IS steering committee should receive the appropriate management information from IS departments, user departments, and audit to coordinate and monitor the institution's IS resources effectively. The committee should monitor performance and institute appropriate action to achieve desired results. Formal minutes of the IS steering committee meetings should be maintained to document the committee's activities and decisions and inform the board of directors of IS activities.

CONTROLS

The development and implementation of controls within an information systems environment is to ensure the accurate, timely, and complete processing of all work. The control environment encompasses the policies, procedures, and organizational structure of the IS function. The examination evaluates the adequacy and effectiveness of the control environment. The following controls should be considered in this evaluation.

Policies and Procedures

Written policies, procedures, and standards provide the basis for establishing and maintaining proper IS controls. Written standards promote uniform implementation of management policies and aid in training new employees. Management must provide policies and procedures for operating units within the IS department. These policies should provide employees of each unit with the necessary guidelines to coordinate and perform their tasks effectively according to the overall policies and procedures of the organization and the IS department. IS policies and procedures should be developed for:

- The acquisition and use of IS resources.
- Computer operations
- Documentation and standards.
- Data entry preparation.
- Computer utilization.
- Programming activities.
- Output report distribution.
- Information systems security controls.
- End-user computing.

- Insurance.
- Financial analysis of vendors.
- Contingency plans.

Standards and procedures should: (1) allow for separation of duties; (2) limit access to valuable assets, e.g., magnetic media, documentation and computer equipment; (3) ensure authorization of all activity within the data processing area; and, (4) provide efficient and effective allocation of resources. Procedures should provide audit trails to ensure that independent controls are implemented by the user departments.

Internal Controls

Management must establish an effective system of internal controls. Internal controls applied to automated systems are often classified into general and application controls.

General controls are part of the information systems environment and include controls over data center operations, system software acquisition and maintenance, access security, and application systems development and maintenance. They apply to all systems, mainframes, minicomputers, and end-user computing. They include control over modification and maintenance of computer programs, operating systems software, and access to applications and data maintained on computer systems.

Examples of general controls are:

- Management controls.
  - Short and long range planning.
  - Policies, standards, and procedures.
  - Organizational structure.
  - Separation of duties.
  - Personnel training.
  - Internal audit.
- Systems Development and Programming
  - Use of systems development life cycle (SDLC) methodology.
  - Program change procedures.
  - System testing.
  - Access controls and security.
- Data Center Operations.
  - Budgets, hardware acquisition plans, and capacity planning.
  - Physical security.
  - Operating procedures.
  - Backup and recovery procedures.
  - Disaster recovery planning.

Application controls are specific to each application. They are designed to detect and correct errors when entering data into the system and protect the integrity of the application software. Application controls ensure the authority of data origination, accuracy of data input, integrity of processing, and verification and distribution of output. Many application controls use computerized edit checks.

Application controls often depend on general controls. Therefore, the adequacy of the general control environment should be determined before analyzing application controls. For example, a general control procedure may protect against unauthorized changes to computer applications. The adequacy of this general control should be determined before reviewing specific application controls relating to the accuracy and reliability of the data.

Examples of application controls are:

- Data preparation/authorization procedures.
- Document counts/control totals.
- Separation of duties for origination, approval, and data entry of documents.
- File identification checks.
- Application level security.
- Programmed edit checks and reasonableness tests.

If a financial institution uses outside service bureaus for data processing services, their controls should be considered. The institution should obtain and review a copy of the service bureau audit report to ensure that appropriate controls exist to process its data and records.

Management Reporting

Management reporting systems that measure the performance of information systems operating units and the data center(s) is another step in the overall

control process. Reporting may be separated for convenience into different functional areas, such as: (1) operations; (2) systems development and programming; and (3) general/personnel. The types of information, frequency, and sophistication of reports will vary depending on the size and nature of the IS department. Examples of information contained in IS management reports are:

Operations

- Reruns per period by application and total run time.
- Incident or failure reports per period broken down by operator, program, or environment type.
- Telecommunications network downtime.
- On-line failures, terminal response time, and percentage of down time per period.
- Internal label overrides by operator per period.
- Out-of-balance conditions on entry runs resulting in adjustments per period.
- Data entry volume per period by operator.
- Special report runs per period.
- Unauthorized terminal/system access attempts.

Management reports must be reviewed promptly for matters that need management's attention. The review can and should be documented by signing and maintaining copies of reports. For microfiche or microfilm output, management may initiate a review log.

Systems Development and Programming

- Programmer time by project or application.
- Systems analyst time by project or application. (Systems analyst and programmer time may be separated into development and maintenance time. An increasing amount of maintenance on an application may indicate that it is near the end of its useful life. Development time may be compared to projection estimates, and in a sophisticated environment, both methods may be useful in a cost accounting system).
- Status reports on system and programming projects that compare current data to projections.

General/Personnel

- Staffing.
- Overtime hours by functional area.
- Late or missorted deliveries per period.

The board of directors and IS management should determine the quality and quantity of report information needed, and the frequency of reports, in monitoring information systems and data center(s) activities. Senior management and the IS steering committee may require monthly or quarterly data, middle management weekly or monthly data, and first-line supervisors daily and weekly data. Typically, senior management reports include a comparison of prior periods with current performance. Adequate financial reporting systems are necessary for the various levels of management control in an IS installation. These reporting systems generally provide department budgets, budget variance, and internal cost accounting information.

Using the management reporting, management should identify deviations or exceptions from expected performance and make necessary modifications. This may be done by periodic management reviews or independent audits. Management controls to improve performance should address significant areas and be economical, since the cost of establishing and maintaining them should not exceed derived benefits. Although establishing controls is the purview of management, the examiners, auditors, and accountants must specify areas in which they are inadequate.

Independent audits, whether performed by internal or external auditors, measure performance and assess independently the adequacy of policies and procedures. An independent audit program provides management with an impartial evaluation of the information systems department condition. Audit reports should cite exceptions and recommend corrective action. The auditors then must follow up to

ensure that corrective action has been taken. Management must review and follow up on exceptions noted and recommendations made in audit and examination reports.

FINANCIAL ANALYSIS

Independent Servicers

A number of financial institutions contract with independent servicers for information processing services. An independent servicer seeks to generate a profit, rather than break even, as does an IS subsidiary of a financial institution holding company, or operate at cost as does an institution's IS department. The importance of monitoring the financial condition of the servicer cannot be overemphasized. Each serviced institution should obtain and analyze carefully annual (preferably audited) financial statements from the servicer. If the servicers financial condition is weak or deteriorating, the serviced institution should plan alternative arrangements and implement them as necessary. Even if the servicer remains in operation, financial problems often lead to drastic cost-cutting measures that may jeopardize the quality of service and data integrity.

Bankruptcy of a data processing servicer can be devastating to a serviced institution. A 60- to 120-day notification of service termination may not be provided. In this situation, the serviced institution – not the servicer – must find an alternative processing site. Although the user institutions can generally obtain current data files from their servicer, the programs and documentation required to process those files are usually owned by the servicer and may not be available to the users. These programs are often the servicer's only significant assets. Therefore, a creditor, in an attempt to recover outstanding debts, might attach a lien to those assets that limits the availability of these programs and documentation to the users. At this point, the serviced institutions could: (1) pay off the creditor and hire outside specialists to operate the center; or (2) convert data files to another servicer. Either of these options would be costly to the users and could cause unacceptable processing delays.

Data Processing Subsidiary/Department

Generally, an IS subsidiary of a holding company does not affect consolidated earnings performance materially, because it usually provides essential services at costs comparable to or below independent servicers. The subsidiary's financial statement should be analyzed to determine operating expenses. Operating efficiencies may result in lower costs for the center and reduced fees for the serviced institutions. However, this may not always be the case. The contracts between the subsidiary and the member financial institutions it services should be reviewed to ensure that the contracts are "arms-length" transactions that are fair and equitable to all parties.

A financial analysis of an IS department should include a comparison of the cost-effectiveness of the in-house operation versus contracting with an outside servicer. It may also include a peer group comparison of operating costs and ratios with similar sized institutions. Depending upon the size of the institution, costs may or may not be allocated to the user departments. Where cost allocation exists, costs should be commensurate with the services provided to user departments. (See Chapter 25, FFIEC issuance SP-6: Interagency Statement on EDP Service Contracts and OTS issuance TB 46: Contracting for Data Processing Services or Systems).

Budget

A final step in the planning process is the development of an operating budget. Management's plans and its success in meeting budgetary goals are assessed to evaluate data processing management, operations, financial conditions, and prospects. The budget review should furnish insight into the organization's future plans and other matters, such as capital adequacy, liquidity, sources and uses of funds, level and quality of earnings, and management's performance.

The budget is a coordinated financial plan used to estimate and control the organization's activities. By assessing future economic developments and conditions, management creates an action plan and records changes in the balance sheet accounts and profitability (predicated on implementation of the plan). The budget, not only projects expected results, but also serves as an important check on management

decisions and performance by providing a basis for comparison with actual performance. A variance indicated by the comparison may measure management's performance and planning record. Significant variances may be caused by factors beyond management's control or those that could not be anticipated. The comparison of actual performance with the budget allows management to consider alternatives and choose one that should result in the greatest benefit.

Budgeting also measures the performance of persons and the departments they manage. The comparison of budget totals to actual performance promotes coordination and cooperation among affiliates. Although various persons may contribute to the budget process, the chief executive officer typically must prepare and implement the formal budget. The budget often is prepared for one year, although it sometimes covers longer periods in larger, more sophisticated IS organizations. The longer the budget period, the greater are the prospects for increased variances from original budget figures. When four or five projections are made, companies may formulate several forecasts based on different sets of assumptions.

In such instances, the examiner should work with the "most likely" situation that may occur based on economic trends, history, and experience of the organization, but also should consider the "worst case" projections.

Many IS organizations, particularly smaller ones, may not have separate written budgets or plans. Budgeting procedures for IS departments should be encouraged.

INSURANCE

In establishing an insurance program, management should recognize its exposure to loss, the extent to which insurance is available to cover potential losses, and the cost of such insurance. These factors should be weighed to determine how much risk the organization will assume directly. In assessing the extent of that risk, the effect of an uninsured loss must be analyzed, not only on the entity that incurs it, but also on the affiliates and the parent. Once appropriate coverage has been acquired, procedures should be established to review the program periodically to ensure the continued adequacy of the coverage. These procedures should include – at a minimum – an annual program review by the board of directors.

Insurance is intended to complement, not replace, an effective system of controls. Thus, an overall appraisal of the control environment becomes significant in assessing the adequacy of the insurance program. Effective controls and audits may result in lower premiums.

Before insurance is purchased, management should assess the costs of insuring:

- IS equipment and facilities.
- Employee fidelity.
- Media reconstruction.
- Extra expense.
- Business interruption.
- Errors and omissions.
- Loss of items in transit.
- Liability to customers resulting from electronic fund transfer systems (EFTS) activities.

Estimates of these costs will enable management to choose the types and amounts of insurance to carry. They also allow management to determine to what extent the institution should self-insure against certain losses.

Management should review periodically and determine the adequacy of insurance coverage for the computer center and equipment outside of the data processing center. If the computer equipment is leased, it should be resolved who is responsible for insurance – the lessor or lessee. If the lessee assumes that responsibility, insurance must be sufficient to cover equipment replacement or unpaid rentals of the equipment.

An institution or data center can insure against risks covered in various standard insurance policies. However, insurance is generally available for physical disasters,e.g., fire and flood often specifically exclude computer equipment. Those policies usually cover replacement of the physical

magnetic media, but omit the cost of reconstructing the recorded information found in the media. Insurance obtained to provide protection against the hazards inherent in a data processing environment is listed in the following sections.

Information Systems Policy

The IS insurance policy is a multiple peril policy designed to provide various types of coverage. It is constructed so that it can be adapted to the particular institution's IS environment. Specific coverage available and evaluation guidelines are:

- *IS Equipment and Facilities* – Provides coverage of physical damage to the data center and owned automation equipment throughout the institution. Insurance on leased equipment should be obtained when the lessee is responsible for hazard coverage.

- *Media Reconstruction* – Covers damage to IS media, such as magnetic tape and disks, which is the insured's property and for which the insured may be liable. Insurance is available for on-premises, off-premises or in-transit situations, and covers the actual reproduction cost of the property or, if not replaced or reproduced, the blank value of the media. Considerations in determining the amount of coverage needed are programming costs, physical replacement, and backup expense.

- *Extra Expense* – Covers the extra costs of continuing operations following damage or destruction at the data processing center or other work areas where IS equipment may be located.

- *Business Interruption* – Provides data centers offering outside services reimbursement for monetary losses resulting from suspension of operations, because of physical loss of equipment or media.

- *Valuable Papers and Records* – Covers actual cash value of papers and records (not defined as media) on insured's premises against direct physical loss or damage.

- *Errors and Omissions* – Provides protection against claims arising from negligent acts, errors, or omissions of the insured that occur in performing IS services for others. These policies commonly contain the following exclusions:

  - Employee dishonesty.
  - Libel, slander, or defamation of character.
  - Liability of others assumed by the insured under contract or agreement.
  - Liability of loss or damage to property of others.
  - Personal or bodily injury or sickness.
  - Liability arising out of advice on methods, procedures, practices, etc.
  - Liability for preparation of income tax returns.
  - Loss caused intentionally by, or at the direction of, the insured.

This type of coverage has become increasingly difficult to obtain and premiums (which are normally based on a percentage of outside processing revenues) are often high. In addition, the method insurance companies use to apply the deductible to a claim varies. For example, if a program error caused an overpayment of interest to 1,000 savings accounts, some policies would apply the deductible to each account rather than to the entire overpayment amount. This method would greatly limit the value of the policy to a financial institution. Servicers must review their operations and the benefit of this type of insurance for their specific needs and exposures.

Fidelity

Bankers Blanket Bonds, excess fidelity insurance, and commercial blanket bonds cover loss from dishonest or fraudulent acts by employees. In a financial institution operating its own data processing facility, fidelity coverage is normally provided under Standard Form No. 24, Bankers Blanket Bond. For off-premises processing arrangements (independent data centers, facilities management groups, affiliates or subsidiaries), fidelity coverage has been extended to include the servicer’s personnel as insured under the Bankers Blanket Bond. To qualify for this coverage, the IS services must be provided under a contract between the servicer and the insured. This additional coverage may be deleted by amendment.

In addition to fidelity coverage provided by the user, independent processors often purchase their own fidelity insurance via a commercial blanket bond. An

independent processor operated as a proprietorship may not be able to include the proprietor under this bond. Therefore, serviced financial institutions must obtain coverage themselves.

Media Transportation

One hazard in off-premises data processing is the potential loss of or damage to items in transit between the data center and the serviced financial institution. The standard Bankers Blanket Bond provides limited coverage under specified conditions. In addition, when media is transported via a hired carrier, the insured can apply for an "interpretive letter" from the blanket bond underwriter extending the coverage to the carrier. Normally, the letter will restrict coverage to nonnegotiable property and to the named carrier.

When media is delivered by mail, special data processing transit coverage is available to financial institutions from only a few underwriters. This insurance is designed to cover the transportation of items to and from an IS center, the cost of reconstruction, and the tracing of lost instruments. This policy usually specifies that the insured must make a copy of all documents covered before they are forwarded to the processor. Coverage includes transportation and dishonesty or collusion by delivery employees. Under policies of this type, coverage usually is not limited to nonnegotiables. This is significant since many nonvoided, nonrestrictive, and negotiable items are sent to outside data facilities.

Wording on transit coverage in the policy usually specifies that all documents must be filmed or otherwise copied. When the policy does not specifically state that data be filmed prior to being transported, and it is not, management should obtain from the insurance carrier a letter that describes the carrier's position and coverage in the event data is destroyed.

Electronic Funds Transfer Systems (EFTS)

To limit the risk associated with EFTS, an institution should review available insurance to determine if there is:

- IS equipment coverage for EFTS equipment located off premises.
- An extension of Bankers Blanket Bond coverage to each Automatic Teller Machine (ATM) on the network.
- Liability insurance coverage for each ATM location.

Insurance coverage at the serviced institution should furnish protection from loss, because of employee dishonesty in the servicer's organization. Standard Form No. 24, "Bankers Blanket Bond," provides fidelity coverage of the data servicer's employees unless specifically excluded by a separate rider. A premium is charged for each processor. Transit Insuring Agreement © of Form 24 covers some of the costs associated with reconstruction of accounts and other records if lost or destroyed during transport by the financial institution's messenger. Additional "Cash Letter," "Valuable Papers," and "Records" coverage may be appropriate.

MANAGEMENT APPRAISAL

Generally, a direct relationship exists between the overall condition of the IS resources and the quality and size of its management and staff. An evaluation of management should consider its performance and planning for future needs.

The examiner should evaluate the staffing, supervision, management responses to correct cited deficiencies from audit and examinations, and control for each area reviewed. Strengths and weaknesses as summarized in the work program (see Chapter 9WP: Management Work Program) should also be considered. Generally, a review of IS in a financial institution or independent service bureau includes a review of financial condition, audit, computer operations, systems development and programming, personnel policies, management succession, and employee training.

Management succession is a legitimate concern of any organization and is perhaps even more important in IS processing. It is to the institution's advantage to employ those who with experience and training could advance to management positions. A financial institution should avoid depending upon one person or several key personnel. Provisions should be made for continuing operations in the event of an unexpected loss of key personnel. Education

programs, including management training for supervisors, can minimize disruptions to operations from management or staff turnover.

Management's ability to administer effectively all aspects of the IS function and to interact with user groups and other managerial personnel within the organization are keys to the success of any data processing operation.

MANAGEMENT INFORMATION SYSTEMS (MIS)

Effective MIS reports are critical to the profitability, success, and long-term viability of each institution. For management and the board of directors to make informed decisions, they must have information systems that provide the necessary information needed to run their business. They must be provided with accurate, timely, and consistent information on the institution's performance, management of its resources, and compliance with regulatory requirements.

A critical factor in reviewing management is the quality of the institution's management information systems. Effective MIS consists of information drawn from a number of sources. Although the concept of quality MIS is accepted widely as a requirement for success, it is difficult to define since MIS requirements are unique to each institution. Examiners should direct their efforts to evaluate MIS by:

- Determining if management has adequately identified information requirements and established effective reporting information to guide their decisions in achieving business goals and measuring performance. Generally, the review of MIS will be facilitated by focusing on a specific safety and soundness concern (i.e., profitability, asset quality, interest rate risk, regulatory reports, such as call reports, thrift financial reports) or compliance issue (i.e., Community Reinvestment Act, and Bank Secrecy Act). The IS examiner must work closely and concurrently with other examiners (e.g., safety and soundness, compliance, trust, or holding company) in reviewing the quality of MIS reporting information at an institution.
- Reviewing MIS reports to determine the accuracy and timeliness of the information provided, and the controls that ensure that it is reliable, timely, accurate, and treated with confidentiality.

Advances in technology have increased the amount of the information available to management and the board of directors for planning and decision-making. These advances have also increased the potential for inaccuracy and errors in management reports. Data may be extracted from numerous transaction and financial systems that run on mainframes, minicomputers, and microcomputers without the benefit of well-designed processing controls commonly found in traditional mainframe systems.

An institution's information requirements depend on its size and the complexity of its operations. Directors and management need information to define goals, guide operations, and make timely decisions. Although examiners should encourage management to develop improved systems and information, they must be reasonable in their expectations. They should encourage institutions to recognize their information needs and take steps to develop the systems to address them.

Management information is required at all levels of the institution. The information at each level may vary according to management's responsibilities. The effectiveness of MIS can be measured in terms of quality, quantity, and timeliness. Examiners must determine if an institution's management information systems provide the type, quantity, and quality of data necessary to assess and monitor its performance.

The following factors may be used to evaluate the quality of the institution's management information systems:

- *Usable* – Decision makers need summarized information. Reports should be designed to eliminate clutter and voluminous details that can create information overload. Care should be taken that board and management reports present only relevant information and do not contain unnecessary detail. The volume of detail in board reports can prevent directors from recognizing potential risks that are more visible in summarized information.

- *Timely* – Current information should be available for decisions. Management information systems should be designed to expedite the reporting of information. Procedures should be designed to collect and edit data, quickly summarize the results, and allow for adjustments and corrections.

- *Accurate* – A sound system of automated and manual internal controls must exist throughout all information systems processing activities. Information should receive appropriate editing, reconcilement, and internal control checks. A comprehensive internal and external audit program helps ensure the adequacy of internal controls.

- *Consisten*t – Data should be processed and compiled the same way each time. Variations in how data is collected and reported can distort information and trend analysis with adverse effects on management decisions. Since data collection and reporting processes change over time, management must establish sound change procedures. The change procedures should be well defined and documented, clearly communicated, and contain an effective monitoring system.

Comments on MIS reports should be specific, rather than general. Management at various levels needs specific information to understand the nature of the deficiency and how to correct it. When making comments examiners should consider :

- Why the MIS report is inadequate. Whether the information provided is timely, is in a useful format, is complete or sufficiently detailed, or is properly organized. Whether the information requires reference to several other sources to be useful.

- That references to specific reports contain a copy of the report with the name and number. Problems are highlighted from the standpoint of the users of the report, not the examiner.

- Whether the report is generated on the mainframe or on a PC within one department. The institution's information systems department cannot fix a report that it does not know exists.

- That if the report is generated within a department, why is it done that way. Whether the accuracy was checked and how.

- Whether the institution has custom report writers and on-line inquiry capability and the audit department commonly uses these programs. The use of custom report writers before the examination can save time during the examination by allowing the examiner, with the help of the institution, to design reports that provide needed information in a useful form.

Because management requires information on economic events that may occur, the use of *models* has become more prevalent. Assumptions made and the quality of information used in models may have a serious effect on the value of the information gleaned from them. Therefore, controls over morels should be sufficient to ensure that management receives accurate information to make proper decisions.

OUTSOURCING DATA PROCESSING SERVICES

The intense competition in the financial services industry has caused institutions actively to seek ways to cut costs and focus on the business of banking. At the same time, the rapid changes in information systems technology have increased the costs of developing and maintaining in-house and end-user information systems significantly. As a result, many financial institutions have contracted with third-party organizations for information processing, telecommunications, item processing, or other selected services. These arrangements generally are referred to as *outsourcing*. Outsourcing is done to reduces operating expenses by removing salary and equipment expenses from the institution's books and allocating the savings in capital to core business needs.

Outsourcing arrangements permit the institution to focus on the business of banking and rely on the servicer to provide state-of-the-art systems in compliance with regulatory requirements. Longer term outsourcing contracts also permit the institution to predict its data processing costs with a higher degree of certainty as the servicer bears the costs of technological changes. The vendor achieves cost

savings and economies of scale by consolidating and reducing data processing facilities, computers, and software maintenance activities. Institutions should ensure that long-term strategic plans are considered in long-term outsourcing contracts.

Outsourcing arrangements generally fall into three categories:

Service Bureau Arrangement

The institution contracts with a servicer to provide data processing systems and services on proprietary software applications used by a number of clients. It may contract out all or some of its applications as it chooses.

Facilities Management (FM)

The institution turns over management of its data center facilities to a third party. The installation is customized to meet its needs. Operating system support is generally the responsibility of the FM provider. The facility housing the computer and the computer equipment is often owned/leased by the institution.

Resource Management

The vendor processes and maintains the institution's software applications at its data center or may install new applications on a dedicated computer. A major difference between a resource management and service bureau arrangement is that, in the latter, the institution uses the vendor provided software applications instead of its own. Current knowledge of software systems is a major factor in outsourcing decisions. Institutions must consider the costs and resources involved in upgrading legacy or early application software systems and maintaining competitive software on mainframe and end-user computing systems.

Outsourcing arrangements often result when management views data processing as one of many functions of the institution. The maintenance of current technology on in-house computer systems may drain profits when institutions are seeking ways to cut costs. Other factors that affect the outsourcing decision may be earnings pressure, possibility of acquisition, internal structuring/decentralization, and the perception that third-party vendors in the information systems business are better equipped to maintain state-of-the-art technology at lower costs. These views are not shared uniformly throughout the financial institutions industry.

A management that pursues outsourcing risks the non-performance of a careful comparison of in-house cost with third-party costs. Review of that analysis leading to the outsourcing arrangement is important for safety and soundness. An evaluation should be made about whether the institution relied solely on the marketing data of vendors or reconciled its system requirements to various outsourcing proposals.

A more difficult area for an institution to evaluate is the cost and benefit of an outsourcing agreement. Some reasons are:

- There are no cost accounting standards in the financial institutions industry. Some institutions spread data processing cost throughout the organization, while others track cost centrally. Thus, the value of any industry data on the average cost of data processing in financial institutions is limited.

- Products and services of outsourcing vendors are priced and packaged differently than in-house data processing operations. Vendor software packages and processing are proprietary and offer different advantages and disadvantages. They are not a homogeneous grouping of products and services and cost comparisons among vendors, and vendors and in-house operations can be misleading (e.g., cost per deposit account).

- The correlation between cost and benefit of an outsourcing agreement is not always identified and quantified. For example, lower data processing costs may be accompanied by higher personnel costs in user departments and lower quality in customer service.

Contracts also should be reviewed carefully by management when considering an outsourcing arrangement. Some considerations are security, ownership of the data stored on vendor media, and the right of the institution to recover its data upon expiration or termination of the contract.

In a typical outsourcing arrangement, the financial

institution signs a contract giving the vendor control of its computer operations for several years. However, the contracts are generally structured, so that the savings for the institution accrue almost entirely during the first few years. Some outsourcing transactions are designed to provide immediate financial relief by having the third party vendor take over the IS equipment and personnel to remove these expenses from the institution books.

The provision of IS services to financial institutions entails certain risks and responsibilities for both the financial institution and the vendor. IS services and systems contracts should address, define, and balance those risks and responsibilities between the vendor and the institution. Guidelines that institutions should consider when contracting for data processing services and systems are provided in the FFIEC issuance SP-6: Interagency Statement on EDP Service Contracts, the OCC issuance BB-87-3: Potential Risks of Long Term EDP Contracts, and the OTS issuance TB-46: Contracting for Data Processing Services or Systems. Additional Serviced Institution Control Guidelines are also provided in Chapter 22.

SYSTEMS CONVERSIONS

Financial institutions must replace periodically existing software applications with new ones developed in-house, or more likely, with vendor software, either through a leasing or outsourcing agreement. The replacement is accomplished through a systems conversion process. These conversions present significant risks of loss to the institution from deficiencies in planning and implementation. Losses incurred often arise from charge-offs resulting from discrepancies between pre-conversion and post-conversion monetary balances, extensive efforts to resolve out-of-balance conditions and to work around unresolved transaction processing deficiencies, and indirectly, negative customer impact. Because individual institutions perform conversions infrequently, its employees do not usually possess conversion expertise. Thus, an inordinately large degree of reliance is often placed on software vendors who, tend to present an over-optimistic view of the effort required to complete a conversion to their system. As a result, conversion-related risks are often increased significantly by implementation efforts performed under unusually tight schedules. Consultants, when engaged, are often hired at relatively short notice. This tends to inhibit their overall effectiveness in guiding the project.

The IS examiner's review should identify potential or actual problems to help avoid loss or major disruption to the institution. It should determine the adequacy of the institution's preparedness for a scheduled systems conversion. To be of most value, the review should be started no sooner than the completion of the planning phase and no later than the middle (approximately) of the user acceptance testing phase. In general, institution management prefers reviews of systems conversions to occur early in the process to take advantage of the reviewer's findings and recommendations. The early detection of significant safety and soundness risk exposures, may be assured by reviewing system conversions in targeted rather than regularly scheduled information systems examinations. This examination may involve in-house data centers, serviced institutions, or service bureaus and should be conducted only by experienced IS examiners.

The IS examination scope is divided into the conversion plan and implementation controls and progress achieved relative to the conversion target date. Each phase has the following features:

- Conversion plan: In most respects, planning for a conversion is similar to that of planning for any systems development effort. All tasks must be identified and executed according to a defined critical path, and personnel and other resource requirements must be provided for to complete the conversion within a designated target date. However, planning for a conversion requires that provisions be made for certain tasks that are uniquely associated with the transfer of processing from one existing system to another. These include file conversion and related balancing procedures, product mapping, data mapping, and the selection of system user options. Planning for these tasks should be reviewed along with that of other tasks that correspond with typical systems development projects including system procedures, user training, and the implementation of disaster recovery planning and information security controls.
- Implementation: An implementation phase review allows examiners to evaluate all aspects of

planning and project management, including an assessment of the progress achieved against task completion target dates. Red flags that portend conditions of high risk exposures include:

Conversion target date:
- Arbitrarily set.
- Management appears firmly opposed to postponement.
- Previous target date(s) missed.
- Conversion team is performing under evident time pressure.

Project management:
- Completion of key tasks and milestones significantly delayed.
- Critical path-dependent tasks are started prematurely (e.g., user acceptance testing is started before the completion of the selection of system user options).
- Project management records are not kept updated.

Testing:
- Planned time frames for testing are shortened.
- The is no evidence of independent review of test scripts for adequacy.
- Deficiencies are identified initially as conversion- critical (show stoppers), are arbitrarily reclassified as noncritical, and are to be corrected after conversion (usually to meet a target date).

Procedures and training:
- Balancing and user procedures are not adequately completed.
- Inadequate progress is made in user training.

Network:
- Network connectivity to the new vendor's facilities is not tested adequately.

EMERGING TECHNOLOGIES

The rapid growth of IS technology is changing business operations in financial institutions. The demand for increased features and functionality of information systems, reliable and timely information, and the reduction of paper have prompted vendors to design a wide range of technical solutions to meet business problems. Advancements in the spread of the Internet, client-server architecture, distributed networks, Fourth Generation Language (4GL) programming languages, storage technologies, expert systems, and electronic data interchange (EDI) have aided the transfer of computing power from centralized computers to end-user computing platforms.

This proliferation of emerging technologies in information processing has created new risk and control issues for the institution and for its regulatory agencies. Institutions are experiencing an increased volume of data, speed of processing, on-line reporting capabilities, complexity of business processes, and user controlled processing. These changes have increased user access to information systems, reduced segregation of duties, caused a shift from paper to electronic audit trail, evolved with a lack of standards and controls for end-user systems, and increased the complexity of corporate contingency and IS recovery planning. Accordingly, the board of directors and regulatory examination personnel must ensure that the risks related to emerging technologies are considered and addressed appropriately by the institution's management. Some emerging technologies that are becoming more prevalent in financial institutions are discussed next.

THE INTERNET

The Internet is the world's largest computer network, but there is no easy way to characterize its size. An estimated 1.2 million computers were connected to the Internet at the beginning of 1993. However, the Internet does not count its membership solely in terms of either computers or computer users. Internet membership also includes networks. Today hundreds of thousands of local networks are connected to the Internet, and its rate of growth is increasing steadily. Roughly 1,000 new networks join the Internet each month. Even new networks do not account for all of the Internet's growth. The Internet's audience expands with every new computer or user that is added to any of its constituent networks.

Origin of the Internet

The Internet had a humble beginning as ARPANET in the early 1970s. The ARPA part of ARPANET stood for Advanced Research Projects Agency (later

called the Defense Advanced Research Projects Agency, or DARPA) of the U.S. Department of Defense (DOD). At the end of the 1970s, other networks sprang into existence. The UUCP (Unix to Unix Copy Protocol) network (a loose confederation of first hundreds and now thousands of UNIX machines) was followed in the early 1980's by BITNET (Because It's Time Network), CSNET (Computer Science Network), and many others. Some were private (such as CERFnet and BITNET), some were collaborative (UUCP), and some were government funded (ARPANET, NSFNET [National Science Foundation], and CSNET). Eventually all of these networks began working together and became known as the INTERNET.

This evolution was begun by the National Science Foundation (NSF), which created a network of interconnected NSF supercomputer sites across the United States in the late 1970s and early 1980s. NSF is a government science agency that connected supercomputer sites to each other to make them more efficient. Scientists, researchers, and engineers could network across the supercomputers and better leverage the agency's computing power.

The high-speed network that connects the NSF supercomputers now forms the backbone of the Internet in the United States. It consists of high-capacity telephone links using microwaves, lasers, fibre optics, and satellites to connect networks, computer sites, and people around the world.

As the Internet has become more visible outside of the research and academic communities, a group of private companies called service providers have evolved. These service providers actually furnish many of the entry point communication lines used by Internet users. Universities, private research labs, and commercial companies rent Internet connections from these providers, as an individual would lease a telephone line from the phone company. The advent of Internet service providers (ISP's) geared to the individual home or small business user community opened up the Internet more fully in the early 1990s.

What Can Be Found on the Internet

The primary growth area for electronic commerce, including banking, is a portion of the Internet called the World Wide Web. The World Wide Web interest commercial enterprises, because it allows users, with necessary navigator software, to display their products graphically and to link to related information merely by pointing and clicking on a highlighted word or phrase.

Searching for information on the Internet is not always easy. There are many tools to help a user find information on the World Wide Web (WWW or The Web) portion of the Internet. These tools, often referred to as browsers, web crawlers, or search engines, allow the user to find topics on the Internet using graphical point-and-click interfaces. The Web puts a friendlier face on the technical aspects of navigating the Internet. The technical complexity of the Internet was a primary reason that it was not noticed much until recently by the public and private enterprise. Currently the most widely used part of the Internet is electronic mail (E-mail).

Organization

The Internet is a loosely structured, informal association of computers connected by networks, whose only mandatory control is the *address* or *network name* of each network site. Without proper controls on the network name, it is not possible to accurately switch or route messages. Therefore, controls on the network name are the fundamental glue that both define and hold the Internet together. The Internet Activities Board (IAB) has this responsibility. The IAB is supported by the Internet Society, a private nonprofit organization of individuals and organizations that are connected to the Internet.

Components

The Internet is comprised of:

- *Computers* – which represent the host locations on the network and can range from a freestanding microcomputer, to a LAN server, minicomputer, or a mainframe.

- *Networks* – which represent the paths over which communications travel between the Internet nodes.

The diversity of hardware and software and the range of processing power of these computers and networks is the source of the Internet strength and its weakness.

Internet Banking

Internet banking creates new challenges. Customer terminals and the delivery channels (e.g., public telephone networks and the Internet) are outside of the institution's control. The global reach of these systems increases the number of uncontrolled points of access to bank computer systems. These attributes introduce heightened security risks and emphasize the need to develop secure systems and procedures for operating in an uncontrolled environment.

An evaluation should be made of risks associated with existing or proposed PC banking programs in terms of all significant technology, legal, regulatory, and economic areas. The following factors warrant special consideration followed by appropriate action:

- *Accountability* – Ensure that proper accounting, audit trails, and operational controls are in place and operating correctly. These controls are normally available in a traditional information systems environment; however, the challenge exists in the ability to monitor and trace the increased transaction volume of more users that accompanies PC banking.

- *Authentication* – Verify the identity of the parties to the transaction. Financial institutions will communicate with customers they may never physically meet and opportunities for misrepresentation will increase. Financial institutions and customers will need a mechanism to verify each other. Authentication is one of the most significant issues related to PC banking.

- *Authorization* – Develop methods, before implementing PC banking, to ensure that customers are authorized access only to their accounts and to perform only pre-determined and legally permissible functions.

- *Capacity* – Acquire and allocate sufficient resources to meet existing and anticipated volume. Customer will expect access to their financial data and the ability to conduct transactions on demand. During peak operating hours, demand may be high and unpredictable.

- *Confidentiality* – Keep customer data safe from unauthorized access. Customer data will be transmitted over public networks. Management must develop methods to maintain privacy.

- *Human Resources* – Ensure there are sufficient trained personnel to supply prompt and expert customer service. All affected employees will need training appropriate to their responsibilities.

- *Information Integrity* – Confirm that data remains accurate and safe from illegal alteration. Customers will enter data in an on-line environment. Management must assure that data transmissions between the customer and the financial institution remain protected from unauthorized viewing or alteration.

- *Non-Repudiation* – Create a system that will provide undeniable proof of participation by both the sender and the receiver of information and data in every on-line transaction. Customers may input data and later deny the transaction took place. Authentication is the primary component of non-repudiation.

- *Outsourcing* – Select only vendors who demonstrate in-depth knowledge and effective use of the emerging technology. Many service bureaus and software vendors will offer to develop and distribute PC banking services. These will include new unproven vendors and established vendors, both of whom may be unfamiliar with the technology and its implications.

- *Reliability* – Ensure that every part of any system used by the bank is available and functions as promised and establish contingency plans for emergencies. Contingency planning is necessary to restore an on-line system that fails and to provide continuity of business activity. Internet reliability is a related concern, but management has little or no control over Internet performance.

- *Software Updates* – Maintain control over software changes. The institution may have to rely on the customer to install software updates. Multiple software versions may have to be supported. The institution must decide what software versions to support and how to accommodate customers unable or unwilling to install updates.

- *Compliance* – Ensure compliance with all legal and regulatory requirements. The existing regulatory framework remains applicable in this emerging technological environment and must be adhered to.

Internet Issues

This area of technology has developed so rapidly that its coverage by current law and regulations is unclear. Many of the laws, rulings, and regulations were under review as we crafted this section. Accordingly, readers should continue to monitor legal developments associated with banking on the Internet. Of particular concern are issues related to error resolution, including: data corruption and

unauthorized transactions; protection of individual privacy; and safeguards against illegal activity. Such safeguards would address particularly the areas of money laundering and fraud.

Actual financial activity on the Internet (or through on-line, services such as America Online, Compuserve, or Prodigy) may take various forms, including:

- Institutions only providing product information on line with referrals to telephone or branch sites for transactions.
- Customers obtaining account status information.
- Customers conducting transactions on existing accounts, (including transferring funds and making payments).
- Institutions providing information about uninsured products and financial planning information.
- Customers initiating the purchase of securities or other uninsured instruments on-line.

Similar services may be delivered through direct dial-up, using branded interfaces provided by the institution or through the use of third-party software, such as provided by Intuit, Microsoft, or MECA.

Numerous issues surround the role of third parties, such as: on-line services, Internet providers, and intermediaries processing financial transactions (such as Intuit, Microsoft, and Checkfree.). Because agent/principal relationships are often defined by applicable state law, no precedent exists for transactions conducted on an interstate or international network by parties whose the geographic location may be unknown. Handbook readers should monitor developments in this area.

Compliance Related Risks and Issues

Internet banking transactions should be subject to the same compliance laws and regulations that apply to "traditional" banking transactions. The application of those laws to Internet banking transactions raises questions, such as compliance with advertising requirements and the provision of timely disclosures in an appropriate form. Financial institutions could risk regulatory enforcement and civil penalties for noncompliance with those laws and regulations.

Depending on the type of transaction that occurs (for example, extension of credit or deposit or withdrawal of funds from an account at a financial institution), the following federal laws and regulations could apply:

- Equal Credit Opportunity Act and Federal Reserve Regulation B

  Prohibits discrimination by creditors in any aspect of a credit transaction on a prohibited basis and requires creditors to provide certain notices concerning credit applications.

- Fair Housing Act

  Prohibits discrimination by any aspect of housing-related lending on a prohibited basis.

- Home Mortgage Disclosure Act and Federal Reserve Regulation C

  Requires depository institutions and mortgage lending institutions to report data on mortgage loan applications, originations, and purchases.

- Electronic Fund Transfer Act and Federal Reserve Regulation E

  Requires financial institutions to provide disclosures and consumer protections (such as error resolution procedures and limitations on liability for unauthorized transfers) concerning electronic fund transfers involving a consumer account.

- Truth in Lending Act and Federal Reserve Regulation Z

  Requires creditors to provide disclosures (including in advertisements) and consumer protections (such as error resolution) in consumer credit transactions.

- Expedited Funds Availability Act and Federal Reserve Regulation CC

  Requires financial institutions to make deposited funds available to customers within specified time frames and to provide disclosures about funds availability policies.

- Truth in Savings Act and Federal Reserve Regulation DD

  Require depository institutions to provide dis-closures (including in advertisements) and consumer protections (such as calculation of interest on the full account balance) concerning deposit accounts.

- Community Reinvestment Act and Federal Reserve Regulations

  Require federal financial regulatory agencies to assess

the record of regulated financial institutions in meeting the credit needs of their entire communities, including low- and moderate-income areas, consistent with safe and sound practices.

To ensure a consistent regulatory policy approach to Internet banking. The following issues should be addressed.

- Appropriate triggers for existing advertising requirements may need to be created for on-line interfaces.

- Standards may need to be set for, if, and when it is appropriate to use on-line disclosures, periodic statements, and notices rather than sending hard copies.

- Similarly, a review may be indicated of the situations in which E-mail communications would appropriately substitute for communications between the institution and a customer.

- Rules for providing disclosures, statements, and notices within certain time frames should be adopted and evaluated for the on-line transmission.

- Whether continuously available real-time statements could substitute for, or issued in lieu of, periodic statements should be considered.

- When downloadable documents and E-mail would be considered a form the customer can retain, as required for certain disclosures, etc. should be resolved.
- Standards should be developed for documents that must be delivered to the consumer, to ensure that they have been received and downloaded both accurately and in their entirety.

Marketing and sale of securities and other uninsured instruments through an institution's Internet site can also potentially raise additional compliance issues.

Institutions have not been sensitive as necessary to the need to separate banking from nonbanking activities, even without direct links to the brokerage provided by Internet browser technology and incorporated into on-line banking interfaces. While the actual securities transactions are covered by SEC rules (which has approved on-line delivery of the prospectus and/or the sale of securities), interface standards should be established to distinguish activities involving uninsured instruments and maintain and reinforce separate corporate identities.

Geographic Issues

Issues related to Internet banking fall into two primary categories: those for institutions using this technology to supplement ordinary banking activities and those for institutions doing business solely on-line.

For the first category of institutions, Internet banking provides an *alternative* delivery system for banking products and services. Access issues may arise over the availability of computers to low- and moderate-income populations. The implications of this are covered in the discussions of automated application systems and retail electronic payment systems. The obvious potential for on-line banking is to concentrate an institution's business in the high end or the market. Furthermore, its geographic independence from an institution's offices provides the potential for an institution to concentrate business outside of its more traditionally identified trade area.

For the second category of institutions, Internet banking provides a *primary* delivery system for banking services. An institution doing business solely on-line could be subject to issues related to computer access by low- and moderate-income segments of a community.

The cornerstone of many laws affecting financial institutions is the concept of a local community, in which the institution is expected to meet the needs of all segments, including those of low- and moderate income persons. Many legislative initiatives address geographic location. Given that an institution doing business on-line could be considered to have an office located wherever any customer has a computer, a different strategy for defining its trade areas may need to be established.

The Internet's Future

The Internet's future as a primary delivery system of financial services is evolving rapidly. Financial institutions using or planning to use the Internet as a financial services delivery mechanism will also continue to develop policies, standards, and procedures internally or collectively to protect their assets and the overall integrity of both their systems and transactions traveling across the Internet.

CLIENT/SERVER COMPUTING SYSTEMS

Client/server networks enable users to share computer resources across all computing platforms of an organization (workstations, PCs, mid-range computers, mainframes). Portions of a single application may be split between the client workstation or PC and the server based on the most effective or efficient use of equipment. A server may be one or more multi-user processors with shared files that serve multiple clients simultaneously to provide printing, facsimile, file storing, database,

computational capabilities, and application processing.

Client/server technology allows organizations to increase worker performance by distributing computing resources and empowering the end user. End users have more input into the design, development, and implementation of new systems. They are now considered to be owners of the data. As owners, they are responsible for data integrity, including security concerns that were only related to the mainframe. In some cases, users of information evaluate, purchase, test, and install powerful programs on their own systems. These user systems may interact with, alter, or replace information processing performed on mainframe computers.

A general area of concern in client/server systems is the adequacy of general computer control procedures. Risk issues in that environment include:

- Data and security issues across platforms in multiple locations with multiple access points.
- Mismanagement of end-user computing.
- Development, maintenance, and testing of new applications.
- Back-up and recovery procedures.
- System integrity affected by lack of controls in end-user platforms.
- End-users inadvertently or deliberately modifying or destroying data.
- High-volume PC use, increasing the possibility of system failure.
- Viruses entering the system.
- Changes in one vendor's hardware affecting other vendor components.

ELECTRONIC IMAGING SYSTEMS

Electronic document imaging systems provide a combination of hardware and software technology to capture, index, store, and retrieve electronic images of paper documents. They are used by financial institutions to reduce paper handling, increase productivity, and improve customer service.

Although the image capture process (scanning) is still in its infancy, the technology is improving and will provide high speed data capture, indexing, reliable optical character recognition, storage, and networked data exchange. Document storage technology is also improving and data storage on write-once-read-many (WORM) and rewriteable optical disks is becoming an integral component of many image systems. The optical disk is a storage device that uses laser technology to retain digitized data from any means of data input, including scanning. The optical storage disk technique is an outgrowth of the demand for higher levels of document storage capacity in a usable form. This new digital media offers a highly reliable and low-cost process for the storage and access of imaged documents and other types of data on a compact optical disk. Imaging systems may streamline department and office workflow processes, reduce storage and retrieval costs, and by automate customer files and correspondence. The replacement of paper documents with electronic images can affect significantly the way an institution does business. Many of the traditional audit and security controls for paper based systems may be reduced or absent in electronic document workflow. New controls must be developed and designed into the automated process to ensure that information in image files cannot be altered, erased, or lost.

Imaging systems generally are grouped into two types: Document management systems and item processing systems. Imaging systems and accompanying risk and controls issues are described in Document Imaging – Chapter 17 and are also referenced in FFIEC SP-10 – Control and Security Issues in Electronic Imaging Systems. This FFIEC policy issuance is located in Chapter 2 of this Handbook.

ELECTRONIC DATA INTERCHANGE (EDI)

EDI refers to the electronic exchange of documents and other data between corporations. Companies exchange documents by direct transmission between computers over telephone lines and data communication links. Data files are transmitted in a standard format that is machine readable by the computer receiving the files. The initial users of EDI were large companies who used communication links and a proprietary transmission format to exchange data with their suppliers and customers. New standard protocols allow customers with different equipment and software to send and receive messages in a standard message format. These messages can be translated and entered directly into the computer system at the destination in an electronic form.

The EDI goals are to lower cost, improve accuracy in billing and inventories, speed cash management, and assure quality control. EDI provides savings in time, postage, and paper by eliminating the mailing of paper documents. It also replaces keying data into a computer from paper documents, at the destination organization,

saving data entry time and reducing keying errors.

The growth of the EDI process has led to the development of transmission standards and value-added networks (VANS). VANS are third-party networks that store and forward messages in a standard format. They serve as electronic mail boxes and provide EDI partners with the flexibility to choose when to access or transmit information. VANS help to reduce scheduling and compatibility problems associated with automated transfers of information between multiple companies.

EDI software generally has three phases: communication, translation, and application interface. A complete message, such as an order invoice, would comprise an EDI transaction. The communication interface transmits the message between the companies or VAN and is designed for error detection and correction to protect against transmission failures. An EDI translator converts the standard EDI messages into proprietary user formats and performs edit checks, response acknowledgments, and validity checks. The application interface converts the information into a format that can be processed by the receiving application software. Usually, the company's software applications are left unchanged.

Financial institutions have been involved primarily with the electronic payment portion of EDI transactions through electronic funds or ACH transfers. These services include wire transfer, automated cash management, and ACH transfer services for the participating companies. The types of ACH transactions involved in the EDI payment process are: prearranged payments or deposits, corporate trade payments, and corporate cash concentration and disbursement transactions. Financial institution customer charges are generally based on a set-up fee, a monthly maintenance charge, and a transaction charge based on the number of characters in EDI transactions.

The greatest risk to financial institutions lies in the electronic payment transaction. Exposures and risk associated with payment system risk apply to EDI transactions. Financial institutions bear a credit risk if payment is made from accounts with uncollected or insufficient funds. Credit limits and transactions caps should be established, periodically reviewed, and strictly enforced.

Since EDI replaces paper with electronic entries, many of the manual process controls are either lost or ineffective. Examples include the substitution of electronic signatures and authorizations to replace written documents. Audit trails, access controls, security and separation of authorization, and execution and data processing functions must be designed into the technology. Backup and restart procedures are necessary to recover operations and assure their continuity. Legal requirements place a need for security and the ability to ensure data integrity. This may require that copies of printed documents be retained to defend against legal suits alleging improprieties in handling the account, or even fraud.

Legal considerations include:

- Proof of authentication.
- Record retention.
- Contract law covering written agreements
- Control regulations stipulated by the Foreign Corrupt Practices Act:
  - Executing transactions in accordance with management's general or specific authorization.
  - Recording transactions to allow for the preparation of financial statements.
  - Controlling access to assets.
- Transactions governed by Federal Reserve's Regulation E.

The following tax regulations and rulings also govern EDI transactions.

- Revenue Ruling 71-20 requires that the media be retained for as long as it would be useful to determine a tax liability.
- Revenue Ruling 86-19 assumes the existence of underlying source documents to support inter-company transaction systems.